



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,010	02/26/2002	Matthew Charles Priestley	MS190438.1	4314

27195 7590 09/16/2005

AMIN & TUROCY, LLP  
24TH FLOOR, NATIONAL CITY CENTER  
1900 EAST NINTH STREET  
CLEVELAND, OH 44114

EXAMINER

ABEDIN, SHANTO

ART UNIT PAPER NUMBER

2136

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/083,010

Applicant(s)

PRIESTLEY ET AL.

Examiner

Shanto Abedin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 02/26/2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>08/02/2002</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

1. Claims 1-33 were presented for examination.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 1-17, and 27-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. For a subject matter to be statutory the claimed invention as a whole must accomplish a practical application. That is must produce a "useful, concrete and tangible result." State Street, 149 F3d at 1373, 47 USPQ2d at 1601-02, MPEP § 2106.

***Regarding claim 1***, it is drawn to a system; all of the elements and features can be implemented in software alone. Therefore the claim is non statutory under 35 U.S.C. 101 as not being tangible. "A wrapper" and "A pass phrase" recited in claim 1 are not tangible.

***Regarding claim 27***, it is drawn to a system; "means" for generating password, passphrase, package, storing password in the package, and locking the package recited in the claim are not tangible. Specification failed to provide any tangible structure associated with the "means" recited in claim 5, it appears that "means" are not limited to

tangible embodiment - could be thought as an application software or could be implemented in software alone - therefore non-statutory.

**Regarding claim 28**, it is drawn to a system; all of the elements and features can be implemented in software alone. Therefore the claim is non statutory under 35 U.S.C. 101 as not being tangible. "Data packet", "A password" and "A wrapper field" recited in claim 28 are not tangible. Furthermore, "A signal" recited in claim 28 is non-statutory as not being tangibly embodied.

**Regarding claim 31**, it is drawn to a system; all of the elements and features can be implemented in software alone. Therefore the claim is non statutory under 35 U.S.C. 101 as not being tangible. "A service", "A pass phrase" and "A wrapper" recited in claim 31 are not tangible. Specification failed to provide antecedent basis for "service" recited in claim 31, it appears that "service" is not limited to tangible embodiment - could be thought as an application software therefore non-statutory.

**Regarding claim 33**, it is drawn to a system; all of the elements and features can be implemented in software alone. Therefore the claim is non statutory under 35 U.S.C. 101 as not being tangible. "A first data field" and "A second data field" recited in claim 33 are not tangible. Furthermore, "A data structure" recited in claim 28 is non-statutory as not being tangibly embodied.

Art Unit: 2136

**Regarding claim 2-17,29, 30 and 32** are rejected under 35 U.S.C. 101 because of their dependencies on the independent claims.

Note: As best understood claim 1-17, 27-33 are examined, and rejected below.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 3,4, 17, 18, 23, 27 – 30, 33 are rejected under 35 USC 102 (b) as being anticipated by Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC" by Lee et. al., EC-Web 2000, LNCS 1875, pp. 63-71, 2000).

**Regarding claim 1, Lee** discloses a system for processing credentials ( Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol) , comprising:

A wrapper (Figure 1, element: Electronic License Packaging) that packages credentials associated with resources of a service (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1: Overall architecture of proposed protocol; Figure 2: Secure installation procedure)[ Lee discloses a merchant server comprising an electronic license packaging module that wraps the software to be downloaded in a package];

A pass phrase ( a “secret” string shared only by authorization unit in client’s computer and by the server, Figure 2, element: Elicense) employed in connection with generation of the wrapper, the pass phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources to the server (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1: Overall architecture of proposed protocol; Figure 2: Secure installation procedure) [ Lee discloses a locked wrapper to package software that can be unlocked using an Electronic License Certificate (ELC) comprising a “secret” component (a random string shared by only the server and authentication module in client’s computer). A person with the ordinary skill in the art will be able to interpret Lee’s “secret” component as a pass phrase].

**Regarding claim 18**, Lee discloses a method to facilitate a security connection between entities (Section 3: Proposed ESD Protocol), comprising:

Generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, passwd) [Lee discloses generation of an electronic license certificate comprising password];

Generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, secret) [Lee discloses generation of an electronic license certificate comprising a "secret" string. The "secret" is shared only between the authentication module and the server and is a random string. A person with ordinary skill in the art would be able to interpret the "secret" as a pass phrase];

Wrapping the password cryptographically via the pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license,  $H(\text{secret}, \text{customer\_ID}, \text{passwd})$ ) [Lee discloses generation of an electronic license certificate also comprising cryptographic function  $H(\text{secret}, \text{customer\_id}, \text{passwd})$  that cryptographically wraps the secret string];

Storing the wrapped password in an executable (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: merchant server, JDBC data source, electronic license processing) [ Lee discloses use of JDBC component, a storing facility and "electronic license packaging" module (which contains password in it) to wrap the packaged software]

**Regarding claim 27, Lee** discloses a system to facilitate a security relationship between parties (Section 3: Proposed ESD Protocol), comprising:

Means for generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, passwd) [Lee teaches generation of an electronic license certificate comprising password in it];

Means for generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, secret) [Lee discloses generation of an electronic license certificate comprising a secret string that works as as a pass phrase];

Means for generating a package ( Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Figure 1, element: Electronic License Packaging ) [Lee discloses a electronic license packaging module to package software in a wrapper]

Means for storing the password in the package (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, H(secret, customer\_ID, passwd); Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee discloses an electronic license certificate (used to package the software) comprising a cryptographic function H (secret, customer\_id, passwd) that securely store the password.]

Means for locking the package with the pass –phrase (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: merchant server, JDBC data source, electronic license processing) [ Lee discloses a H function (as a part of electronic license certificate)



comprising a password, and a pass phrase like "secret" string that is used to lock the wrapper containing packaged software]

**Regarding claim 28**, Lee discloses a signal to communicate security data between at least two nodes ( Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme; Figure 1, element: electronic license packaging; figure 2: E license) comprising: a first data packet comprising:

A password component employed to establish a trust relationship between at least two nodes (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, Figure 2, element: E-license, H(secret, customer\_ID, passwd) [Lee discloses an electronic license certificate which contains a cryptographic function H (secret, customer\_ID, passwd) comprising password in it];

A wrapper field employed to encapsulate the password, the wrapper field mediating access to the password (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1, element: Electronic license packaging; Figure 2, element: e-license) [Lee discloses generation of an electronic license certificate which contains a cryptographic function H (secret, customer\_id, passwd) which cryptographically secure the password. A person with the ordinary skill in the art would be able to design a wrapper field to encapsulate the password by using similar technique used by Lee to form H (secret, customer\_id, passwd)]

**Regarding claim 33, Lee** discloses a computer readable medium having stored thereon a data structure (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Fig 2, element: e- license; Fig 3, element: executable packaged file, decryption of encrypted exe file and software execution thread), comprising:

A first data field (password field of H function) containing cryptographic data associated with a password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Fig 2, element: e- license) [ Lee discloses an electronic certificate comprising hash function  $H(\text{secret}, \text{customer\_id}, \text{passwd})$  where password is encrypted using MD5 or SHA cryptographic algorithm.]

A second data field (secret field of H function) containing cryptographic data associated with a pass phrase, the pass phrase employed to migrate exposure of the password to non trusted entitie (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Fig 2, element: e- license) [Lee discloses an electronic certificate comprising hash function  $H(\text{secret}, \text{customer\_id}, \text{passwd})$  where secret is a pass phrase like random string (cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996.) . Password is cryptographically secured within the H function.]

**Regarding claim 3, Lee** discloses the credentials providing stronger encryption than the pass phrase ( Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme) [ Lee discloses that second component of the electronic license certificate (that implies to credentials) are encrypted by using a public key and server's private

Art Unit: 2136

key. A person with the ordinary skill in the art can conclude that this type of public and private key encryption is usually stronger (128 bit or more) than the random string (recited in Lee) or the key crunching algorithm (usually 64 bit encryption) to generate random string from the pass phrase or a secret string (cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996).]

**Regarding claim 4, Lee** teaches that credentials are encrypted with greater than 100 bits of encryption ( Section 1: Introduction, Paragraph 3; Section 3.1: Overall Architecture, Paragraph 2; Section 3.2: Secure Installation scheme, Paragraph 1)[ Lee teaches use of encryption schemes such as Diffie Hellman, RSA, MD5, and SHA – all of them usually use greater than 100 bits of encryption (recited in cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996).]

**Regarding claim 17, Lee** discloses a computer readable medium having computer executable instructions stored thereon to perform at least one of processing and generation of the wrapper and the pass phrase ( Section 2.2: Software based technologies; Section 3.1: Overall architecture; Figure 1, element: electronic license packaging) [ Lee teaches use of JDBC component "electronic license packaging" to package and email the wrapped electronic license (which contains a "secret" string as pass phrase) to customer.]

**Regarding claim 23,** Lee discloses a method of limiting access to the executables (Section 2.2: Software based technologies; Section 3.3: Illegal copy protection mechanism; Figure 3: Illegal copy protection protocol using multi thread). [ Lee teaches use of an authentication server to limit access to the executable packages]

**Regarding claim 29,** Lee discloses a wrapper field being cryptographically weaker than the password ( Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme) [ Lee discloses that password and other credentials in electronic license certificate are encrypted by using a public key and server's private key. A person with the ordinary skill in the art can conclude that this type of public and private key encryption is usually stronger (128 bit or more) than the random string (recited in Lee) or the key crunching algorithm (usually 64 bit encryption) to generate random string from the pass phrase or a secret string (used for wrapper field) (cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996).]

**Regarding claim 30,** Lee discloses a system of claim 28. Lee further discloses a second data packet containing a pass phrase to unlock the wrapper (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, secret) [Lee discloses generation of an electronic license certificate comprising a secret string as a pass phrase and using such secret string as a means of unlocking the wrapped package];

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claim 2, 5-11, 19, 20, 26 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al ("A secure electronic software distribution (ESD) protocol based on PKC" by Lee et. al., EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Ramakrishnan ("Java based E-commerce middleware" by Sub Ramakrishnan, 2001 IEEE)

***Regarding claim 2, 19 and 26, Lee*** discloses a system for processing credentials comprising a wrapper and a pass phrase of claim1 and sending the electronic certificate which contains wrapper and pass phrase through email (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol). Lee also discloses a electronic license certificate (which contains pass phrase like "secret" string in it) to unlock the wrapped executable package (Section 2.2:Software based technologies, Figure 3, element: executable packaged file).

Lee does not disclose expressly that the pass phrase is distributed separately from the credentials. However, Ramakrishnan teaches a users' typed in pass phrase (serializable object) to be used in encryption wrapper algorithm to secure credentials (Section 2: A middleware E-commerce application; Section 3: Implementation Issues; Figure 5: Process for transmission of encrypted serializable objects.)

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Ramakrishnan to distribute the pass phrase used in wrapper algorithm separately from the credentials by typing in or using email. The motivation for doing so would been to provide added content security in e-commerce communication. (Ramakrishnan, Section 2: A middleware E-commerce application, Paragraph 1.)

***Regarding claim 5 and 9, Lee discloses a system of claim 3 (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme).***

Lee does not disclose expressly that the pass – phrase having human readable, and alpha – numeric characteristics. However, Ramakrishnan teaches a pass phrase that can be typed in by user - which inherently teaches to be spoken, displayed on a screen, readable by human, and alpha – numeric ( Section 2: A middleware E-commerce application, Paragraph 1.)

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Ramakrishnan to design a pass phrase that is human readable, alpha – numeric and can be displayed on the screen. The

motivation for doing so would simply been that such human readable and alpha numeric pass phrase is convenient for client's use and could be generated from either client or server side conveniently and efficiently.

**Regarding claim 6, 7, and 8,** Lee discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee does not disclose expressly that one or more partners request access to the resources, or partners store and distribute the credentials. However, Ramakrishnan teaches web hosting services where web servers work as partners or third parties to request, store, or distribute credentials to the clients from an original server (Section 1: Background, Paragraph 4; Figure 3: Process flow and application component)

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Ramakrishnan for utilizing a pass phrase base wrapper for credential security in a system involving multiple partners facilitating users' need. The motivation for doing so would been that content and original server confidentiality are highly desirable in Internet (WAN) based system.

**Regarding claim 10, 11,** Lee discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee does not disclose expressly use of that pass phrase over a SSL connection or in a VPN environment. However, Ramakrishnan teaches web hosting services where web client talks to the web server using a secure, SSL, connection (Section 1: Background, Paragraph 4 and 5).

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Ramakrishnan for utilizing a pass phrase base wrapper for credential security in a system involving SSL connection or VPN. The motivation for doing so would been that a SSL connection or VPN provides further content security while transmitted through a network.

***Regarding claim 12*** is rejected applied as above rejecting claim 11, furthermore Lee discloses issuing an Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) by merchant server, and obtaining a public key certificate from a third party Certificate Authority (Section 3.1: Overall architecture, Figure 1, element CA) to facilitate secure communication between merchant server and customer.

***Regarding claim 20*** is rejected applied as above rejecting claim 19.

Lee does not expressly teaches a pass phrase to unlock a strong password. However, Ramakrishnan discloses a pass phrase based encryption/ decryption mechanism to lock/ unlock a password (section 2: A middleware e-commerce application; section 3: Implementation issues; Figure 5; Process for transmission of



Art Unit: 2136

encrypted serializable object). Ramakrishnan teaches a pass phrase based encryption mechanism and a cipher engine (Section 3: Implementation issues; Figure 6, element: simpleDESEncryptAndDecrypt() class.

At the time of invention, it would have been obvious to a person with the ordinary skill in the art to combine the teaching of Lee with Ramakrishnan for implementing a unlocking mechanism similar to Ramakrishnan's cipher engine (employing pass phrase based encryption and decryption) in order to securely unlock a strong password.

5. Claims 13 – 16, 21, 22, 31, and 32 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC" by Lee et. al., EC-Web 2000, LNCS 1875, pp. 63-71, 2000) as applied to claim 1 above, in view of Brainard ( " SecurSight: An overview for secure information access" by John G. Brainard, RSA Laboratories)

**Regarding claim 31,** Lee discloses a system to establish a trust relationship, comprising:

A wrapper generated by the service to package the credentials (Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1, element: Electronic License Packaging, producer, merchant server)[ Lee discloses a wrapper generated by merchant server (associated with a producer module) to package software];

A pass phrase employed to generate the wrapper and mediate access to the service ((Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1: Overall Architecture of proposed protocol) [Lee teaches a secret string within an electronic license certificate which is used to lock the wrapper containing packaged software, and such certificate is used to mediate access to the resources]

Lee does not disclose expressly a service that controls one or more resources, and service issues credentials to facilitate access to the resources. However, Brainard teaches a security services comprising a manager module that issues Privilege Attribute Certificates to facilitate desktop's access to the resources.

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Brainard for designing a service which issues credentials to mediate users' access to the resources. The motivation for doing so would be that issuing of credentials as means of authenticating users is commonly practiced in secure client/ server content retrieval systems.

***Regarding claim 13 and 14, Lee discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).***

Lee does not disclose expressly a platform provisioning service, or such service being associated with a partner including a service provider and tenant. However, Brainard teaches a system of SecurSight authentication service which includes a manager, application server, client desktop, and directory services for external

Art Unit: 2136

resources (Section 1.1: SecurSight Design Principal; Section 1.2: Component; Section 3: Authorization; Figure 5: PAC Usage). A person with ordinary skill in the art can design a platform provisioning service by using similar technique used in Brainard's manager component (that will act as both the authentication service and as the long term repository for users' access rights) of the SecurSight authentication service. A person with ordinary skill in the art can also implement a system comprising provisional services, client, and service provider by using similar technique used in Brainard's system consist of manager, desktop, and application server (Figure 5: PAC usage). Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions.

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Brainard for designing system of claim 1 further comprising platform provision service, partners, and service providers in order to facilitate network or enterprise application/ resources to the users efficiently and securely.

**Regarding claim 15** is rejected applied as above rejecting claim 14, furthermore Lee discloses a "secret" string as a part of Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) that is used to unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1; Section 3.2: Secure Installation scheme, Paragraph 2) .

**Regarding claim 16** is rejected applied as above rejecting claim 14, furthermore Lee discloses a system associated with ecommerce technology (Section 1: Introduction, Paragraph 1 and 2) and use web browser to present the credentials to the client (Section 4: Comparison with existing models, Table 1) that is used to unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1;Section 3.2: Secure Installation scheme, Paragraph 2).

**Regarding claim 21**, Lee discloses a system of claim 18.

Lee does not expressly teaches requesting a secure socket layer (SSL) connection or presenting an SSL certificate in response to the request. However, Brainard teaches requesting a secure socket layer(SSL) connection ( Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service) and presenting an SSL certificate in response to the request(Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[ Brainard teaches a desktop requesting for SSL connection with application server, and presenting a certificate to certificate validation service for validation.]

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Brainard for using a SSL connection and using a SSL certificate for authentication purpose. The motivation for doing so would been that SSL connection and use of SSL certificates are commonly practiced in secure network communication.

**Regarding claim 22** is rejected applied as above rejecting claim 21, furthermore Brainard teaches a method comprising at least one of:

Verifying an SSL certificate (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[ Brainard teaches an application access agent and a certificate validation service to validate SSL certificates];

Requesting a Universal Resource Locator (URL) from a listener( Section 2.4: Comparison with other authenticators)[ Brainard teaches obtaining web browser based credentials which essentially refers to use of an URL] ;

Presenting authentication credentials to a receiver (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[ Brainard teaches desktop presenting a certificate to be validated by the certificate validation service.];

Logging in a caller to an account (Section 3.1: PAC definition; Section 3.3: use of PACs by connect agents) [ Brainard teaches a connect agent that initiates a client's access to an account after certificates are validated.]

**Regarding claim 32** is rejected applied as above rejecting claim 13, 14, 15 and 31 [ Brainard discloses a manager module that perform as provisioning service, and issues credentials to authenticate users to access resources (Section 1.1: SecurSight Design Principal; Section 1.2: Component; Section 3: Authorization; Figure 5: PAC Usage)].

6. Claim 24 and 25 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC" by Lee et. al., EC-Web 2000, LNCS 1875, pp. 63-71, 2000) as applied to claim 18 above, in view of Chatani et al ( Pub No: US 2002/0104019 A1)

***Regarding claim 24, Lee discloses a system of claim18.***

Lee does not expressly discloses a method of setting up account privileges or designing account contacts or verifying the contacts. However, Chatani discloses method comprising at least one of:

Setting up account privileges (Fig 2B: element 224: User Info, element 240: Purchase info; Fig 1, element 102; Page 3, Paragraph [0027]; Page 6, Paragraph [0048] and [0049]) [ Chatani teaches a user account to store necessary users' and purchase information in server that are used to authorize the resources. Person with ordinary skill in the art can use a similar technique as Chatani's to set up an account privileges method];

Designating account contacts (Fig 2B: element 224: User Info; Page 6, Paragraph [0048] and [0049]) Chatani teaches storing necessary user information in server. Person with ordinary skill in the art can store account contact using Chatani's teachings];

Verifying the contacts (Fig 2B: element 224: User Info; Page 6, Paragraph [0045], [0048] and [0049]) [ Chatani teaches a server to verify user's purchase

information. A person with ordinary skill in art can use a similar technique as Chatani's to verify the contacts ].

At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Lee with Chatani for setting up an account privileges and verifying the contact associated with that account. The motivation for doing so would be that user authentication is highly desirable in secure network communication.

***Regarding claim 25*** is rejected applied as above rejecting claim 24.

Lee does not expressly disclose a method of verbally communicating the password. However, Chatani discloses a method comprising verbally communicating the password (Figure 3A, element 314; Page 3, Paragraph [0025]; Page 5, Paragraph [0037], Paragraph [0038], Paragraph [0041]) [Chatani teaches using a telephone for inputting alphanumeric ID and for transmitting voice commands]

A person with ordinary skill in the art would modify the system of Lee with Chatani to verbally communicate the pass phrase in order to provide an alternative means for communicating the password and to maintain reliability of the system.]

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- "Applied Cryptography" by Bruce Schneier, Second edition, Wiley, 1996

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for



Art Unit: 2136

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

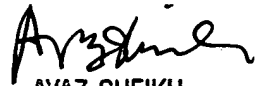
For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M. Z. Abedin

Art Unit: 2136



AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100